Secure AI innovation at scale

Security for AI with Cisco AI Defense

AI adoption is skyrocketing — but so are the risks. From shadow AI to adversarial attacks, enterprises face a new frontier of threats. Through our strategic partnership with Cisco, NTT DATA has created an integrated approach to security for AI. By combining our full AI lifecycle security services with Cisco's AI Defense platform, we offer end-to-end visibility, protection and assurance.

Together, we empower enterprises to embrace AI innovation safely and confidently.

You're adopting AI, but fears of bias, data leakage and attacks are slowing adoption. Proving compliance and building trust remain difficult. We close that gap by combining AI risk and compliance frameworks with Cisco's AI-native defenses to reduce regulatory and reputational risk. We build trust into your AI systems from the start, integrating governance, assurance and runtime protection so you can innovate securely and at scale.

End-to-end coverage

NTT DATA protects the full AI lifecycle (design, build, deploy, monitor), while Cisco AI Defense secures AI-infused applications and shadow AI usage in real time.

Holistic assurance

With Cisco's built-in technical guardrails, including prompt injection defense, AI firewalls and data-leakage prevention, and expert-led governance through NTT DATA's services, you'll be compliant with ISO/IEC 42001, National Institute of Standards and Technology (NIST) AI RMF, and the EU AI Act.

> "We empower you to move faster, scale AI-powered innovation securely, and avoid reputational, financial and legal risks."

Our integrated approach

NTT DATA's Security for AI Services

- **AI Risk and Compliance Service**
  Assessments and AI lifecycle governance aligned with ISO/IEC 42001, NIST AI RMF and global regulations
- **AI Protection Service**
  Defense of AI models, data, applications, APIs and GenAI environments
- **AI Assurance Service**
  Continuous red teaming, structured large language model (LLM) testing and adversarial simulation
- **Secure AI Lab**
  A turnkey innovation and testing environment with built-in partner integrations
- **Engagement models**
  Readiness assessments, adoption, managed services and on-demand red teaming

Cisco's AI Defense capabilities

- **AI cloud visibility**
  Discovers and inventories AI workloads, models and data flows across cloud environments
- **AI access**
  Control employee AI usage to prevent data leaks
- **AI model and application validation**
  Identifies vulnerabilities in AI models and applications early in development
- **AI supply chain risk management**
  Secures models, datasets and dependencies from external sources against compromise
- **AI runtime protection**
  Real-time threat blocking for AI workloads

Protect AI and your business

Secure innovation at scale

Evaluate AI use cases and run secure proofs of concept (POCs) faster with NTT DATA's Secure AI Lab, preconfigured with Cisco AI Defense capabilities. This shortens time to value by accelerating deployment from months to weeks.

Experimental AI playground

NTT DATA's Secure AI Lab Center of Excellence (CoE) Service brings a turnkey Security for AI experimental playground to enterprises designed to rapidly learn, experiment and define security for enterprise AI use cases.

Trusted compliance and governance

NTT DATA's assurance services align your AI programs with global standards such as ISO/IEC 42001 and the NIST AI RMF. Backed by Cisco's continuous threat model updates, this reduces legal risks and helps you avoid costly fines and reputational damage.

Uncover hidden AI risks

NTT DATA's AI Red Teaming service combines industry-leading tools, a proprietary framework, and a rich library of pre-validated adversarial use cases to proactively uncover hidden AI risks and ensures continuous AI assurance.

Shadow AI risk management

We proactively discover unauthorized AI tool usage and apply policies that prevent data leaks. This reduces hidden risks while supporting the secure adoption of new AI tools.

Real-time defense for production AI

We protect your production AI workloads with layered guardrails, AI firewalling and intelligent policy enforcement

Contact us to learn more.

> "Together, we enable safe, scalable and resilient AI adoption that drives innovation and growth."

Visit nttdata.com to learn more.

NTT DATA is a global innovator of digital business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have experts in more than 70 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.

